Université de Bretagne Occidentale

Comment choisir un mot de passe robuste

Sommaire

1. La sécurité par mot-de-passe

Un mot-de-passe sert généralement à **protéger l'accès à une ressource** : l'ouverture d'une session sur un réseau (e.g session Windows), l'accès au contenu d'un fichier (e.g Excel), l'utilisation d'une application (e.g SIFAC).

Il est toujours **personnel** et ne doit jamais être **partagé**. En effet, lorsqu'un mot-de-passe est partagé :

- Il devient impossible de déterminer qui l'a utilisé pour réaliser une action.
- Nous oublions que nous l'avons partagé un jour et nous continuons à l'utiliser pour protéger des données dont nous ne voudrions pas qu'elles soient connues de tiers.
- Si nos propres actions sont sous notre contrôles, celles d'un tiers – quel qu'il soit – ne le sont pas.
- Il convient de ne pas confondre confiance et angélisme.

Un attaquant va essayer de découvrir ce mot-de-passe en testant toutes les combinaisons possibles ou en l'obtenant directement ou indirectement auprès de l'utilisateur.

Un mot-de-passe robuste est donc un mot-de-passe difficile à :

- **deviner** par un tiers,
- **casser** par un système de craquage (« password crackers »).

Un mot-de-passe efficace allie une dernière qualité : il est facile à **retenir** par son utilisateur.

Dans la suite de ce document, nous allons vous présenter quelques méthodes pour créez votre propre mot-de-passe. Vous trouverez également plusieurs chapitres plus techniques sur la sécurité et les faiblesses des mots-de-passe.

2. Créer un mot-de-passe efficace

Sur le plan technique, un mot-de-passe robuste :

- Fait au moins 12 caractères,
- Comprend des lettres majuscules et minuscules, accentuées ou non, des chiffres et des caractères spéciaux ($%,;&…),

- Sa composition ne respecte aucune règle évidente et prévisible pour un tiers.

Exemple : P$é&c;7v!15T3

Mais un tel mot-de-passe reste difficile à mémoriser et conduit souvent son propriétaire à en conserver une trace écrite (Post-It, carnet, etc.), ce qui constitue un risque important de divulgation.

Pour être aisément mémorisé, ce mot-de-passe doit avoir une signification pour vous : cette association mnémotechnique vous permettra de le retenir.

Nous vous proposons deux méthodes simples pour cela :

2.1 Une combinaison de mots rares

Cette méthode combine plusieurs mots rarement utilisés et sans lien entre eux.

1. Choisissez des mots rares car ils sont souvent inconnus des applications pirates. Privilégiez des mots accentués encore moins fréquents dans un environnement dominé par l'anglais.
   Par exemple : ecclésiaste pléistocène
2. Convertissez quelques lettres en majuscule selon votre propre règle (la 2ème lettre de chaque mot, par exemple) : eCclésiaste pLéistocène
3. Puis reliez les mots par un chiffre et/ou un caractère spécial.
   Dans notre exemple : eCclésiaste7%6pLéistocène
4. Pour corser le tout, vous pouvez ajouter quelques fautes d'orthographe… pour peu que vous vous en souveniez.
   Par exemple : eCcléziaste7%6pLéystocène

Si cet exemple vous semble trop long à saisir, choisissez des mots plus courts mais toujours peu fréquents.

2.2 Une phrase improbable

Choisissez une phrase ou expression qui n'aura de sens que pour vous.

Un exemple : 2 * 3 = 5 (c'est mathématiquement faux mais le propos n'est pas là !)

Altérez-là : 2 fois 3 font 5

Puis insérez des variantes et caractères spéciaux.

Au final : 2foiS3!fonT5

2.3 Autres méthodes

Il existe une infinité d'autres méthodes. L'essentiel est que celle que vous choisirez vous permette de mémoriser un mot de passe robuste (difficile à deviner et à casser).

Voici quelques exemples :

Expression de départ (mnémotechnique)	Étapes de la transformation	Mot-de-passe final
ma maison est bleue	ma maison & bleue m9a m8aison & b7leue m9A m8Aison & b7Leue	m9Am8Aison&b7Leue
un été torride	1 été torride 1 été to2Ride 1-été-to2Ride	1-été-to2Ride

un tiens vaut mieux que deux tu l'auras	1 tiens vaut mieux que 2 tu l'auras 1Tvmq2tl'a (10 caractères) 1Tvmq2tl'a34 (12 caractères)	1Tvmq2tl'a34

Quelques conseils :

- Privilégiez des mots contenant des caractères accentués français et donc généralement absents dans les autres langues.
- Adoptez des règles de transformation faciles à retenir mais sans logique évidente (par exemple : 1ère lettre du 1er mot en majuscule, puis 2e lettre du 2e mot en majuscule, etc.)

2.4 Contre-exemples

Voici des exemples de mots-de-passe à ne pas choisir ainsi que leurs faiblesses.

(ces exemples sont fictifs mais basés sur des cas réels)

Mots-de-passe faibles	Faiblesses
19560420	Trop court. Date de naissance aisée à casser en quelques secondes.
princesse8	Trop court. Mot courant.
jacqlesn29	Structure trop simple : prénom/nom/département
ettouspourun	« et tous pour un » Mots trop courant. Absence de caractères majuscules, accentués ou spéciaux.

3. Comment fonctionnent les mots-de-passe ?

Un mot-de-passe est constitué d'une suite de caractères alphanumériques : caractères minuscules et majuscules, accentués ou non, chiffres et caractères spéciaux (&%?!, etc.)

Depuis de nombreuses années, les mots-de-passe ne sont plus stockés en clair sur les systèmes informatiques mais le sont sous une forme codée non réversible : on parle de signature ou de « hash ».

Exemples :

Mot-de-passe en clair	Signature stockée
1-été-to2Ride	cb499ba04295921945224262f1a89de84b99e94628f5f8cd96f0f949d2d43d3a56d0a5e2ce3d8fb578b59a08613785ecbe509e9e1097ee4c08cbada51c9455f2
1Tvmq2tl'a34	f7b3ff161fb7b319d83600b5fa615318bddc113fa00ecbb0b8147f5f7c40f1195679621a2cfb750ad3a93d94706591f0ab3b631c83d87604ca0ecacb35e593fb

Lorsque l'utilisateur entre son mot-de-passe en clair pour s'authentifier, ce dernier est codé pour former une nouvelle signature. Cette signature est alors comparée à celle stockée sur le système : si les signatures correspondent, l'accès est autorisé.

Si tout ou partie de la « base des mots-de-passe » d'un système informatique est divulguée et connue d'un tiers malveillant, aucun des mots-de-passe ne lui est pourtant directement accessible : pour chaque signature récupérée, il doit retrouver la chaîne de caractère en clair (le mot-de-passe).

Le principe d'un « bon » mot-de-passe est que cette opération lui soit la plus difficile possible.

4. Compromettre un mot-de-passe

Compromettre un mot-de-passe revient à en prendre connaissance, généralement à l'insu de son propriétaire.

Il existe plusieurs manières de compromettre un mot-de-passe :

1. Par force brute : en essayant toutes les combinaisons possibles.
2. Par utilisation d'un dictionnaire : à partir d'une grande liste de mots, tester toutes les combinaisons possibles et leurs variantes.
3. Par ciblage : à partir des nom et prénom de la personne, de sa date de naissance, de son lieu d'habitation, du nom de ses proches ou de son animal de compagnie, etc., tester les quelques combinaisons possibles.
4. Par tromperie : en incitant la personne à le divulguer elle-même (cf. hameçonnage et ingénierie sociale).
5. Par cheval de Troie : en installant un virus sur le poste de l'utilisateur et en captant toutes les saisies au clavier (« keylogger »).

4.1 Casser un mot-de-passe

Les trois premières méthodes font appel à du matériel informatique devenu standard : un logiciel spécialisé (mais librement disponible) va tester toutes les combinaisons possibles d'une suite de caractères jusqu'à retrouver celle qui correspond à la signature ciblée.
La puissance des matériels actuels du marché rend cette opération aisée si le mot-de-passe est « trop court » ou trop simple.

Pour donner un ordre d'idée, une carte graphique GTX 1050 TI sortie en octobre 2016 (et coûtant 140€ environ en janvier 2020), permet de calculer 130 millions de signatures par seconde.
Un mot-de-passe de 6 caractères alphanumériques sera ainsi révélé en moins de 7 minutes. Pour 8 caractères, il lui faudra moins de 8 heures. Cela prendra 8 jours maximum pour un mot-de-passe de 10 caractères et 61 ans pour un de 12 caractères[1].

En 2020, un mot-de-passe doit donc faire au **minimum 12 caractères** (mais il peut être plus long !) pour espérer résister aux matériels disponibles.

5 Les attaques par ingénierie sociale et hameçonnage

L'ingénierie sociale est une large gamme de techniques visant à récupérer de l'information par manipulation psychologique[2]. Dans le contexte de la sécurité informatique, elle consiste à inciter un utilisateur à révéler lui-même son mot-de-passe ou toute autre information confidentielle.

Elle est souvent utilisée lorsqu'un pirate n'a pas accès à la base de signatures des mots-de-passe ou lorsque les mots-de-passe sont trop robustes pour être cassés rapidement.

Nous évoquerons quelques techniques communément utilisées en 2020 :

5.1 Ingénierie sociale par téléphone

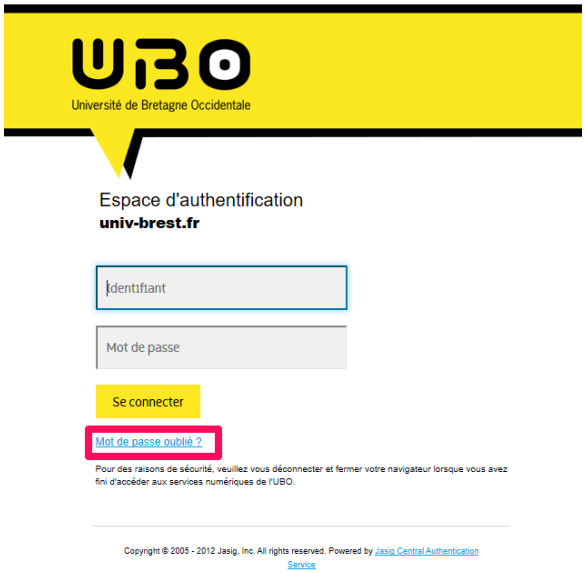
Dans cette attaque, une personne vous contacte par téléphone en se faisant passer pour un collègue ou une autorité quelconque. Elle vous demande des informations sur vous, vos fonctions, le nom de vos collègues directs et leurs fonctions.

[1]Source : https://www.pivotpointsecurity.com/blog/password-strength-explained/ (en anglais)
[2]Réf.: https://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_(s%C3%A9curit%C3%A9_de_l%27information)

Fort de ces informations, elle rappellera le service informatique et se fera passer pour vous ou l'un de vos collègues. Expliquant qu'elle a oublié son mot-de-passe, elle demandera qu'il soit changé et que le nouveau lui soit communiqué par téléphone.

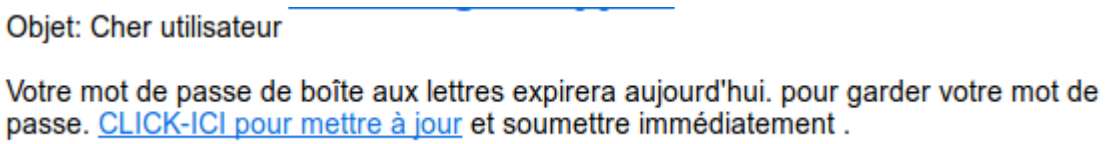
C'est pour cette raison que les agents de la DSIUN ne vous demanderont ni ne vous communiqueront jamais un mot-de-passe par téléphone ou par mail.

Depuis janvier 2020, vous disposez d'une application accessible sur l'ENT vous permettant de générer un nouveau mot-de-passe en cas de perte du précédent :



5.2 Hameçonnage

L'hameçonnage fait partie des techniques d'ingénierie sociale. Dans sa forme la plus courante, elle prend la forme d'un email vous incitant fortement à vous connecter immédiatement sur un système prétendument légitime :



Dans cet exemple, le lien renvoie sur une page imitant la page de connexion de l'UBO.

Si vous rentrez vos identifiants sur cette page, ceux-ci seront communiquez au pirate et vous serez renvoyé sur le site légitime de l'UBO, vous laissant croire à une erreur de saisie lors de votre authentification.

Si un tel cas se présente, il n'est pas trop tard pour agir (vite) :

- Changez immédiatement votre mot-de-passe à partir de l'ENT,
- Informez votre assistant de proximité afin que les tentatives de connexion à votre compte soient surveillées par la DSIUN pendant quelques jours.